RECEIVED
CENTRAL FAX CENTER
OCT 31 2007

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method for calculating hashing of a message in a device communicating with a smart card, comprising:

determining the message to hash ~~storing a same hash function in said device and said smart card~~, wherein the message is divided in data blocks, [[and]] wherein the message comprises a key[[s]] and public data ordered in a sequence, and wherein the key[[s]] [[are]] is only known by the smart card;

hashing, using a hash function, ~~performing a calculation of the hash function of~~ the key[[s]] in the smart card to obtain a hashed key; [[and]]

hashing, using a hash function, ~~performing the calculation of the hash function~~ at least a portion of the ~~of all or part of other data of the message in the device, wherein the other data is~~ public data in the device to obtain hashed public data,

wherein the hashed key and the hashed public data are used to obtain a hash of the message,

wherein hashing the key comprises applying the hash function to the key when the key proceeds, based on the sequence, the public data in the message;

wherein hashing the key comprises applying the hash function to the key and the hashed public data when the key follows, based on the sequence, the public data in the message;

wherein hashing the public data comprises applying the hash function to the public data when the public data proceeds, based on the sequence, the key in the message;

wherein hashing the public data comprises applying the hash function to the public data and the hashed key when the public data follows, based on the sequence, the key in the message.

2. (Cancelled)

3. (Canceled)

4. (Canceled)

5. (Currently Amended) An apparatus comprising:

a communication device configured to be coupled to a smart card, said communication device and said smart card storing a same hash function for calculating a hash of a message, said message being divided in data blocks and comprising a key[[s]] and public data, wherein the key[[s]] [[are]] is only known by the smart card,

wherein said communication device includes a program for performing the following steps:

a first hashing step in which ~~all or~~ at least a part of said public data is hashed in said communication device to obtain hashed public data, [[and]]

a first requesting step in which, said communication device requests the smart card to perform the calculation of the hash function of the key[[s]] using the key and the hashed public data, wherein the result of the calculation is a hash of the message,

a second requesting step in which said communication device requests the smart card to perform the calculation of the hash function of the key to obtain a hashed key, and

a second hashing step in which at least a part of said public data is hashed in said communication device using the public data and the hashed key, wherein the result the hash of the message,

wherein the first hashing step and the first requesting step are performed when the public data proceeds the key in the message, and

wherein the second hashing step and the second requesting step are performed when the public data follows the key in the message.

6. (Cancelled)

7. (Currently Amended) An system comprising:

a smart card; and

a communication device configured to be coupled to said smart card, said communication device and said smart card storing a same hash function for calculating a hash of a message, said message being divided in data blocks and comprising a key[[s]] and public data, wherein the key[[s]] [[are]] is only known by the smart card,

wherein said communication device includes a program for performing the following steps:

a first hashing step in which ~~all or~~ at least a part of said public data is hashed in said communication device to obtain hashed public data, and

a first requesting step in which, said communication device requests the smart card to perform the calculation of the hash function of the key[[s]] using the key and the hashed public data, wherein the result of the calculation is a hash of the message,

a second requesting step in which said communication device requests the smart card to perform the calculation of the hash function of the key to obtain a hashed key, and

a second hashing step in which at least a part of said public data is hashed in said communication device using the public data and the hashed key, wherein the result the hash of the message,

wherein the first hashing step and the first requesting step are performed when the public data proceeds the key in the message, and

wherein the second hashing step and the second requesting step are performed when the public data follows the key in the message, and

wherein said smart card includes a program for performing, ~~upon a~~ responsive to the first request from said communication device, calculation of the hash function of the key using the key and the hashed public data[[s]] ~~of the message~~ and, responsive to the second request from said communication device, calculation of the hash function of the key.